CLAIMS

What is Claimed is:

Sub A2

1. A method of operating a computer system, said method comprising:

providing a first version of a program in memory, said first version of a program including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data; and

performing a first verification including verifying said program prior to execution of said program, said first verification including

indicating a verification error when a first version of a first program unit implementation is not internally consistent;

indicating a verification error when said first version of said first program unit implementation is inconsistent with a first version of said first program unit API definition file associated with said first version of said first program unit implementation;

receiving a second version of said first program unit implementation and a second version of said first program unit API definition file, said second version being a revised version of said first version;

performing a second verification including verifying said second version of said first program unit implementation, including

indicating a verification error when said second version of said first program unit implementation is not internally consistent; and

indicating a verification error when said second version of said first program unit implementation is inconsistent with said second version of said first program unit API definition file; and

performing a third verification including verifying said second version of said first program unit implementation is binary compatible with said first version of said first program unit implementation by comparing said first version of said first program unit API definition file and said second version of said first program unit API definition file.

2. The method of claim 1, further comprising:

indicating a verification error when a second program unit implementation that references said first program unit is inconsistent with said first version of said first program unit API definition file; and

indicating said second program unit implementation is verified with said second version of said first program unit API definition file when said second version of said first program unit binary is compatible with said first version of said first program unit implementation.

3. The method of claim 2, further comprising:

indicating said second program unit implementation is verified with said second version of said first program unit implementation when said second program unit implementation is verified with said second version of said first program unit API definition file.

4. The method of claim 1 wherein said first version of said first program unit API definition file is binary compatible with said second version of said first program unit API definition file when said second version of said first program unit API definition file includes a superset of each element in said first version of said first program unit API definition file.

5. The method of claim 1 wherein

said first program unit references items in at least one other program unit; and

said second verification includes indicating a verification error when said second version of said first program unit implementation is inconsistent with API definition files of each referenced program unit.

6. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform program verification, comprising:

providing a first version of a program in memory, said first version of a program including at least one program unit, each program unit comprising an Application

Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data; and

performing a first verification including verifying said program prior to execution of said program, said first verification including

indicating a verification error when a first version of a first program unit implementation is not internally consistent;

indicating a verification error when said first version of said first program unit implementation is inconsistent with a first version of said first program unit API definition file associated with said first version of said first program unit implementation;

receiving a second version of said first program unit implementation and a second version of said first program unit API definition file, said second version being a revised version of said first version;

performing a second verification including verifying said second version of said first program unit implementation, including

indicating a verification error when said second version of said first program unit implementation is not internally consistent; and indicating a verification error when said second version of said first program unit implementation is inconsistent with said second version of said first program unit API definition file; and

performing a third verification including verifying said second version of said first program unit implementation is binary compatible with said first version of said first program unit implementation by comparing said first version of said first program unit API definition file and said second version of said first program unit API definition file.

7. The program storage device of claim 1, further comprising:

indicating a verification error when a second program unit implementation that references said first program unit is inconsistent with said first version of said first program unit API definition file; and

indicating said second program unit implementation is verified with said second version of said first program unit API definition file when said second version of said first program unit binary is compatible with said first version of said first program unit implementation.

8. The program storage device of claim 2, further comprising:

indicating said second program unit implementation is verified with said second version of said first program unit implementation when said second program unit implementation is verified with said second version of said first program unit API definition file.

9. The program storage device of claim 1 wherein said first version of said first program unit API definition file is binary compatible with said second version of said first program unit API definition file when said second version of said first program unit API definition file includes a superset of each element in said first version of said first program unit API definition file.

10. The program storage device of claim 1 wherein

said first program unit references items in at least one other program unit; and

said second verification includes indicating a verification error when said second version of said first program unit implementation is inconsistent with API definition files of each referenced program unit.

11. A system for executing a software application, the system comprising:

a computing system that generates executable code, comprising means for providing a first version of a program in memory, said first version of a program including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data; and

means for performing a first verification including verifying said program prior to execution of said program, said first verification including

means for indicating a verification error when a first version of a first program unit implementation is not internally consistent;

means for indicating a verification error when said first version of said first program unit implementation is inconsistent with a first version of said first program unit API definition file associated with said first version of said first program unit implementation;

means for receiving a second version of said first program unit implementation and a second version of said first program unit API definition file, said second version being a revised version of said first version;

means for performing a second verification including verifying said second version of said first program unit implementation, including

means for indicating a verification error when said second version of said first program unit implementation is not internally consistent; and

means for indicating a verification error when said second version of said first program unit implementation is inconsistent with said second version of said first program unit API definition file; and

means for performing a third verification including verifying said second version of said first program unit implementation is binary compatible with said first version of said first program unit implementation by comparing said first version of said first program unit API definition file and said second version of said first program unit API definition file.

12. The system of claim 11, further comprising:

means for indicating a verification error when a second program unit implementation that references said first program unit is inconsistent with said first version of said first program unit API definition file; and

means for indicating said second program unit implementation is verified with said second version of said first program unit API definition file when said second version of said first program unit binary is compatible with said first version of said first program unit implementation.

13. The system of claim 12, further comprising:

means for indicating said second program unit implementation is verified with said second version of said first program unit implementation when said second program unit implementation is verified with said second version of said first program unit API definition file.

14. The system of claim 11 wherein said first version of said first program unit API definition file is binary compatible with said second version of said first program unit API definition file when said second version of said first program unit API definition

file includes a superset of each element in said first version of said first program unit API definition file.

15. The system of claim 11 wherein

said first program unit references items in at least one other program unit; and

said second verification includes means for indicating a verification error when said second version of said first program unit implementation is inconsistent with API definition files of each referenced program unit.

16. A resource-constrained device, comprising:

memory for providing a remotely verified application software program comprising at least one program unit, each program unit comprising type specific instructions and data, said remote verification utilizing an Application Programming Interface (API) definition file for each said implementation, each said API definition file defining items in its associated program unit that are made accessible to one or more other program units, said remote verification including verifying a second version of a first program unit implementation is binary compatible with a first version of said first program unit implementation by comparing said first version of said first program unit API definition file and said second version of said first program unit API definition file; and

a virtual machine that is capable of executing instructions included within said application software program.

17. The resource-constrained device of claim 16 wherein said resource-constrained device comprises a smart card.

18. The resource-constrained device of claim 17 wherein said virtual machine is Java Card™-compliant.